LECTURE NOTES ON ARTIN–TITS GROUPS

PATRICK DEHORNOY

updated: July 17, 2004

Contents

Artin–Tits groups are Coxeter groups with torsion removed (but, in the general case, no proof that they are torsion free is known...); they are also generalized braid groups, according to the equation

$$\frac{\text{Artin–Tits groups}}{\text{Coxeter groups}} = \frac{\text{braid groups}}{\text{symmetric groups}}, \text{ which also reads } \frac{\text{Artin–Tits groups}}{\text{braid groups}} = \frac{\text{Coxeter groups}}{\text{symmetric groups}}.$$

Not much is known in the general case. The only well-understood case is the spherical case, *i.e.*, when the associated Coxeter group is finite. Even more results are known in the case of braids, *i.e.*, when the associated Coxeter group is a symmetric group.

0.1. **Braid groups.** In terms of transpositions, the symmetric group S_n admits the presentation

$$(0.1) \qquad \langle \sigma_1, \ldots, \sigma_{n-1} \,;\, \sigma_i^2 = 1,\ \sigma_i\sigma_j = \sigma_j\sigma_i \text{ for } |i-j| \geqslant 2,\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \text{ for } |i-j| = 1\rangle.$$

When the torsion relations $\sigma_i^2 = 1$ are removed, one obtains *Artin's braid group* B_n:

$$(0.2) \qquad \langle \sigma_1, \ldots, \sigma_{n-1} \,;\, \sigma_i\sigma_j = \sigma_j\sigma_i \text{ for } |i-j| \geqslant 2,\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \text{ for } |i-j| = 1\rangle,$$

investigated by Emil Artin [1, 2]; braids have been mentionned by Gauss seemingly, and by Hurwitz certainly. Braid groups have a very rich theory. One of the reasons that makes them popular is that they admit (a number of) nice geometric definitions. The simplest one involves braid diagrams.

The principle is to associate with every word in the letters $\sigma_i^{\pm 1}$ a plane diagram by concatenating the elementary diagrams of Figure 1 corresponding to the successive letters. Such a diagram can be seen as a plane projection of a three-dimentional figure consisting on n disjoint curves connecting the points

1991 *Mathematics Subject Classification.* 20F36.
Key words and phrases. Artin group, braid group.

$(1,0,0), \ldots, (n,0,0)$ to the points $(1,0,1), \ldots, (n,0,1)$ in $\mathbf{R}^3$, and, then, (0.2) is a translation of ambient isotopy, *i.e.*, the result of continuously moving the curves without moving their ends and without allowing them to intersect. It is easy to check on Figure 2 that each relation in (0.2) corresponds to an isotopy; the converse implication, *i.e.*, the fact that the projections of isotopic three-dimentional geometric braids always can be encoded in words connected by (0.2) was proved by E. Artin.

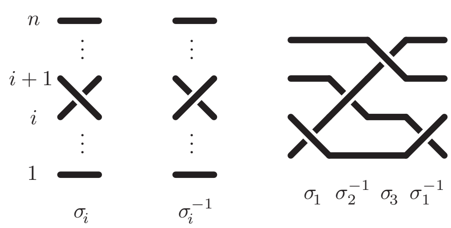


FIGURE 1. Braid diagrams associated with σ_i, σ_i^{-1}, and with $\sigma_1\sigma_2^{-1}\sigma_3\sigma_1^{-1}$

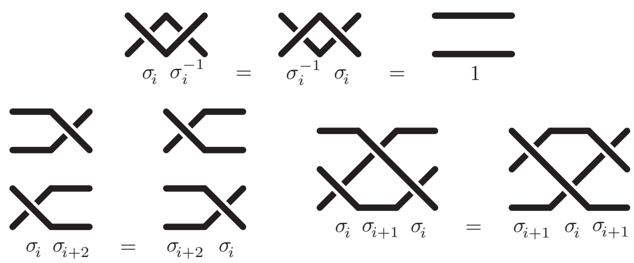


FIGURE 2. Geometric interpretation of the braid relations: in each case, the involved diagrams are projection of isotopic 3D figures

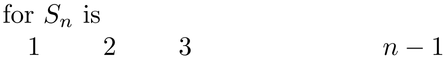
The geometric interpretation makes it clear that mapping the braid σ_i to the transposition $(i, i+1)$ induces a surjective homomorphism $\pi : B_n \to S_n$. Under π, a braid b is mapped to the permutation f of $1, \ldots, n$ such that the strand that finishes at position i begins at position $f(i)$ in some/any diagram associated with b. The kernel of π is the normal subgroup of B_n generated by the braids σ_i^2 and their conjugates (the pure braids)—a counterpart to the fact that S_n admits the presentation (0.1).

0.2. **Artin–Tits groups.** On the shape of S_n, *Coxeter groups* are defined by presentations of the form

$$\langle \{\sigma_i \,;\, i \in I\};\ \sigma_i^2 = 1,\ \mathrm{prod}(\sigma_i, \sigma_j, m_{i,j}\rangle = \mathrm{prod}(\sigma_j, \sigma_i, m_{j,i})), \tag{0.3}$$

where $\mathrm{prod}(x, y, m)$ stands for $xyxy\ldots$, m letters, and $m_{i,j}$ is a positive integer with $m_{i,j} \geqslant 2$, and $m_{i,j} = m_{j,i}$. Note that, when the torsion relations $\sigma_i^2 = 1$ are present, the relation $\mathrm{prod}(\sigma_i, \sigma_j, m_{i,j}) = \mathrm{prod}(\sigma_j, \sigma_i, m_{j,i})$ is equivalent to $(\sigma_i\sigma_j)^{m_{i,j}} = 1$.

For instance, S_n corresponds to choosing $I = \{1, \ldots, n\}$ and $m_{i,j} = 2$ for $|i - j| \geqslant 2$ and $m_{i,j} = 3$ for $|i - j| = 1$. All the needed data can be stored as the list of the indices $m_{i,j}$, hence as a so-called *Coxeter matrix*, *e.g.*, $\begin{pmatrix} 1 & 3 & 2 \\ 3 & 1 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ for the group S_4. An alternative way is to draw a *Coxeter graph* with one vertex for each generator, and one (unoriented) edge labelled $m_{i,j}$ between the vertices σ_i and σ_j; the conventions are that 2-labeled edges are skipped, and 3-labelled edges are represented unlabelled. Also, one allows the case when there is no relation between σ_i and σ_j, and one considers that it corresponds to $m_{i,j} = \infty$. The Coxeter graph for S_n is



When we start with a Coxeter presentation, *i.e.*, equivalently, with a Coxeter matrix, or with a Coxeter graph, and remove the torsion relations $\sigma_i^2 = 1$, one obtains a new group presentation

$$\langle \{\sigma_i \,;\, i \in I\};\ \mathrm{prod}(\sigma_i, \sigma_j, m_{i,j}) = \mathrm{prod}(\sigma_j, \sigma_i, m_{j,i})\rangle : \tag{0.4}$$

this is what is called the *Artin group* associated with the Coxeter presentation/matrix/graph. Artin groups have been investigated by Jacques Tits in the 1960's as "generalized braid groups" (but never by Artin), which makes it reasonable to call them *Artin–Tits groups*.

So, for instance, B_n is the Artin–Tits group corresponding to the symmetric group S_n.

Definition. For Γ a Coxeter graph, we denote by
- Σ_Γ the associated set of generators, *i.e.*, the vertices of Γ;
- R_Γ the associated Artin–Tits relations, *i.e.*, the relations defined by the weights of the edges in Γ;
- A_Γ^+ the associated Artin–Tits group, *i.e.*, the group $\langle \Sigma_\Gamma \,;\, R_\Gamma \rangle$;
- A_Γ^+ the associated Artin–Tits monoid, *i.e.*, the monoid $\langle \Sigma_\Gamma \,;\, R_\Gamma \rangle^+$;
- W_Γ the associated Coxeter group, *i.e.*, the quotient of A_Γ obtained by adding all relations $\sigma_i^2 = 1$.

Remark. One often calls *Coxeter system* a pair (W, Σ) consisting of a Coxeter group W together with a generating family of reflections (order 2 elements); such datum determines a presentation unambigously, and, therefore, one Artin–Tits group. If we just start with a Coxeter group W, it is not *a priori* obvious that different Coxeter systems for W lead to the same Artin–Tits group: proving this requires to find a more intrinsic definition of the Artin–Tits group from the Coxeter group (it exists).

1. The general case

What can one say about an Artin–Tits group starting from its presentation? Not much in general... In good cases, there is a satisfactory theory, originating from Garside's work on B_n [32]. Here we address the question using *word reversing*, a general combinatorial method for studying presented groups [23, 24], which is relevant for establishing properties like cancellativity or embeddability in a group of fractions.

1.1. **The word reversing technique.** For Σ a nonempty set (of letters), we call Σ-*word* a word made of letters from Σ, and $\Sigma^{\pm}$-*word* a word made of letters from $\Sigma \cup \Sigma^{-1}$, where Σ^{-1} is a disjoint copy of Σ containing one letter σ_i^{-1} for each σ_i in Σ. Then Σ-words are called positive, and we say that a group presentation (Σ, R) is *positive* if R exclusively consists of relations $u = v$ with u, v nonempty positive words. We use $\langle \Sigma \,;\, R \rangle$ for the group and $\langle \Sigma \,;\, R \rangle^+$ for the monoid defined by (Σ, R). Note that an Artin–Tits presentation is positive—but a Coxeter presentation is not: a relation $x^2 = 1$ is not allowed..

Definition. Let (Σ, R) be a positive group presentation, and w, w' be $\Sigma^{\pm}$-words. We say that w is *right R-reversible* to w', denoted $w \curvearrowright_R w'$, if w' can be obtained from w using finitely many steps consisting either in deleting some length 2 subword $\sigma_i^{-1}\sigma_i$, or in replacing a length 2 subword $\sigma_i^{-1}\sigma_j$ by a word vu^{-1} such that $\sigma_i v = \sigma_j u$ is a relation of R.

Right R-reversing uses the relations of R to push the negative letters (those in Σ^{-1}) to the right and the positive letters (those in Σ) to the left by iteratively reversing $-+$ patterns into $+-$ patterns. Note that deleting $\sigma_i^{-1}\sigma_i$ enters the general scheme if we assume that, for every letter σ_i in Σ, the trivial relation $\sigma_i = \sigma_i$ belongs to R.

Left R-reversing is defined symmetrically: the basic step consists in deleting a subword $\sigma_i\sigma_i^{-1}$, or replacing a subword $\sigma_i\sigma_j^{-1}$ with $v^{-1}u$ such that $v\sigma_i = u\sigma_j$ is a relation of R.

Example 1.1. Consider the presentation (0.2). Let $w = \sigma_3^{-1}\sigma_1\sigma_2^{-1}\sigma_1$. Then w contains two $-+$-subwords, namely $\sigma_3^{-1}\sigma_1$ and $\sigma_2^{-1}\sigma_1$. So there are two ways of starting a right reversing from w: replacing $\sigma_3^{-1}\sigma_1$ with $\sigma_1\sigma_3^{-1}$, which is legal as $\sigma_1\sigma_3 = \sigma_3\sigma_1$ is a relation, or replacing $\sigma_2^{-1}\sigma_1$ with $\sigma_1\sigma_2\sigma_1^{-1}\sigma_2^{-1}$, owing to the relation $\sigma_1(\sigma_1\sigma_2) = \sigma_1(\sigma_2\sigma_1)$. In any case, iterating the process leads in four steps to $\sigma_1\sigma_1\sigma_2\sigma_3\sigma_2^{-1}\sigma_3^{-1}\sigma_1^{-1}\sigma_2^{-1}$. The latter word is terminal since it contains no $-+$ subword. It is helpful to visualize the process using a planar diagram similar to a Van Kampen diagram as shown in Figure 3.

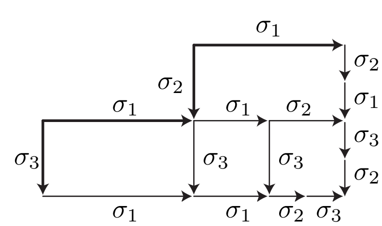


Figure 3. Right reversing diagram for $\sigma_3^{-1}\sigma_1\sigma_2^{-1}\sigma_1$: one starts with a staircase labelled $\sigma_3^{-1}\sigma_1$ and $\sigma_2^{-1}\sigma_1$ by drawing a vertical σ_i-labelled arrow for each letter σ_i^{-1}, and an horizontal σ_j-labelled arrow for each positive letter σ_j. Then, when $\sigma_i^{-1}\sigma_j$ is replaced with vu^{-1}, we complete the open pattern corresponding to $\sigma_i^{-1}\sigma_j$ into a square by adding horizontal v-labelled arrows and vertical u-labelled arrows.

If $\sigma_i u = \sigma_j v$ is a relation of R, then $\sigma_i^{-1}\sigma_j$ and vu^{-1} are R-equivalent, hence $w \curvearrowright_R w'$ implies that w and w' represent the same element of $\langle \Sigma \,;\, R \rangle$. A slightly more careful argument shows that, if u, v, u', v'

are positive words, then $u^{-1}v \curvearrowright_R v'u'^{-1}$ implies that uv' and vu' represent the same element of $\langle \Sigma\,; R\rangle^+$. So, in particular, if u, v are positive words, $u^{-1}v \curvearrowright_R \varepsilon$ (the empty word) implies that u and v represent the same element of $\langle \Sigma\,; R\rangle^+$. The converse need not be true in general, but the interesting case is when this happens:

Definition. A positive presentation (Σ, R) is said to be *complete for right reversing* if right reversing always detects positive equivalence, *i.e.*, for all Σ-words u, v, one has $u^{-1}v \curvearrowright_R \varepsilon$ whenever u and v represent the same element of $\langle \Sigma\,; R\rangle^+$.

Symmetrically, we say that $(\Sigma; R)$ is complete with respect to left reversing if uv^{-1} is left R-reversible to ε whenever u and v represent the same element of $\langle \Sigma\,; R\rangle^+$. The point is that there exists a tractable criterion for recognizing whether a given presentation is complete for reversing—or for adding new relations if it is not.

Definition. A positive presentation (Σ, R) is called *homogeneous* if there exists an R-invariant mapping λ from Σ-words to $\mathbf{N}$ satisfying $\lambda(\sigma_i) \geqslant 1$ for every σ_i in Σ, and $\lambda(uv) \geqslant \lambda(u) + \lambda(v)$ for all Σ-words u, v.

If all relations in R preserve the length of the words, then the length satisfies the requirements for the function λ and the presentation is homogeneous: this is the case for all Artin–Tits presentations.

Proposition 1.2. *A homogeneous positive presentation (Σ, R) is complete for right reversing if and only if the following condition holds for each triple $(\sigma_i, \sigma_j, \sigma_k)$ of letters:*

$$\sigma_i^{-1}\sigma_j\sigma_j^{-1}\sigma_k \curvearrowright_R vu^{-1} \quad \text{with } u, v \text{ positive implies} \quad v^{-1}\sigma_i^{-1}\sigma_k u \curvearrowright_R \varepsilon. \tag{1.1}$$

Condition (1.1) is called the *right cube condition for* $(\sigma_i, \sigma_j, \sigma_k)$. A symmetric left cube condition guarantees completeness for left reversing.

Lemma 1.3. *For each Coxeter graph Γ, the presentation $(\Sigma_\Gamma, R_\Gamma)$ is homogeneous and satisfies the right and left cube condition, hence it is complete for right and left reversing.*

1.2. **Artin–Tits monoids.** Once a presentation (Σ, R) is known to be complete for reversing, some results can be established easily. We begin with results involving the monoid.

Lemma 1.4. *Assume that (Σ, R) is a positive presentation that is complete for right reversing. Then $\langle \Sigma\,; R\rangle^+$ is left cancellative whenever R contains no relation of the form $\sigma_i u = \sigma_i v$.*

There is no relation of the form $\sigma_i u = \sigma_i v$ or $u\sigma_i = v\sigma_i$ in R_Γ, so we deduce:

Proposition 1.5. *Each Artin–Tits monoid admits left and right cancellation.*

Let us now consider common multiples. Say that z is a least common right multiple, or right lcm, of two elements x, y in a monoid M if z is a right multiple of x and y, *i.e.*, $z = xx' = yy'$ holds for some x', y', and every common right multiple of x and y is a right multiple of z.

Lemma 1.6. *Assume that (Σ, R) is a positive presentation that is complete for right reversing. Then a sufficient condition for any two elements admitting a common right multiple to admit a right lcm is that, for all σ_i, σ_j in Σ, there is at most one relation of the form $\sigma_i u = \sigma_j v$ in R. In that case, for all Σ-words u, v, the word $u^{-1}v$ is right reversible to a word of the form $v'u'^{-1}$ with u', v' positive if and only if the elements represented by u and v in $\langle \Sigma\,; R\rangle^+$ admit a common right multiple, and then uv' represents the right lcm of these elements.*

By construction, there is at most one relation $\sigma_i u = \sigma_j v$ in an Artin–Tits presentation; hence:

Proposition 1.7. *Any two elements x, y of an Artin–Tits monoid admit a right lcm if and only if they admit a common right multiple if and only if, for u, v any positive words that represent x, y, the right reversing of $u^{-1}v$ converges in a finite number of steps.*

(Say that the right reversing of w *converges* if there exist positive words u, v satisfying $w \curvearrowright uv^{-1}$.)

Corollary 1.8. *Any two elements of an Artin–Tits monoid admit a left and a right gcd.*

It remains to study whether common multiples do exist. This need not be the case, but, at least, one has sufficient conditions:

Lemma 1.9. *Assume that (Σ, R) is a positive presentation that is complete for right reversing. Then a sufficient condition for any two elements to admit a common right multiple is that there exists a set of positive words $\widehat{\Sigma}$ that includes Σ and is closed under right reversing, in the sense that, for all u, v in $\widehat{\Sigma}$, there exist u', v' in $\widehat{\Sigma}$ satisfying $u^{-1}v \curvearrowright v'u'^{-1}$.*

If there exists a finite set $\widehat{\Sigma}$ as above, then a computer can find it. In the case of Artin–Tits groups, a direct answer will come from the study of Coxeter groups and the following obvious criterion:

Lemma 1.10. *Assume that M is a monoid generated by Σ and*

$$(\mathcal{C}) \qquad (\exists \widetilde{\Sigma} \supseteq \Sigma)(\forall x, y \in \widetilde{\Sigma})(\exists x', y' \in \widetilde{\Sigma})(xy' = yx').$$

Then any two elements of M admit a common right multiple.

We write $(\mathcal{C}^{fin})$ for $(\mathcal{C})$ with the additional requirement that the involved set $\widetilde{\Sigma}$ is finite.

Proposition 1.11. *Assume that A_Γ^+ is an Artin–Tits monoid satisfying $(\mathcal{C})$. Then any two elements of A_Γ^+ admit left and right lcm's and gcd's. If, moreover, $(\mathcal{C}^{fin})$ is satisfied, then word reversing solves the word problem of the monoid in quadratic time and linear space.*

Proof. Reversing solves the word problem only if its always converges. Under the hypotheses of the proposition, there exists a finite set of words $\widehat{\Sigma}$ satisfying the conditions of Lemma 1.9. □

1.3. **Artin–Tits groups.** In good cases, namely when Condition $(\mathcal{C})$ holds, we deduce results for the group.

Lemma 1.12 (Ore). *Assume that M is a cancellative monoid and any two elements of M admit a common right multiple. Then M embeds in a group of right fractions, i.e., there exists a group G in which M embeds and that is every element of G admits a decomposition xy^{-1} with x, y in M.*

Proposition 1.13. *Assume that A_Γ^+ is an Artin–Tits monoid satisfying Condition $(\mathcal{C})$. Then A_Γ^+ embeds in A_Γ, and A_Γ is a group of left and right fractions of A_Γ^+.*

Under the previous hypotheses, word reversing solves the word problem for the group.

Proposition 1.14. *Assume that A_Γ^+ is an Artin–Tits monoid satisfying Condition $(\mathcal{C})$. Then a word w represents 1 in A_Γ^+ if and only if its double right reversing ends up with an empty word, where double right reversing consists in right reversing w into uv^{-1} with u, v positive, and then right reversing $v^{-1}u$. If $(\mathcal{C}^{fin})$ is satisfied, the complexity of the algorithm is quadratic in time and linear in space.*

There are many case when $(\mathcal{C})$ is false. In such cases, the previous results about the monoid do not say anything about the group. In particular, it is not clear whether the monoid embeds in the group.

Theorem 1.15 (Luis Paris, [49]). *For every Coxeter graph Γ, the Artin–Tits monoid A_Γ^+ embeds in the group A_Γ.*

The proof consists in proving that the monoid A_Γ^+ always admits a (possibly infinite–dimensional) linear representation by extending the Lawrence–Krammer representation of B_n [37, 38].

When $(\mathcal{C})$ is not satisfied, *i.e.*, when word reversing need not converge, it is not clear that the word problem of the group is solved by (multiple) word reversing, in any sense.

Definition. Say that a word w is *reversible* to w' if one can transform w into w' using finitely right and left reversing steps, as well as positive and negative equivalences consisting in replacing some positive (*resp.* negative) subword w_0 with an equivalent positive (*resp.* negative) word w_0'. Say that reversing solves the word problem of a presentation (Σ, R) is every word representing 1 is reversible to the empty word.

Question 1.16. *Does reversing solve the word problem of every Artin–Tits presentation?*

1.4. **Exercises.**

Exercise 1.1. (*) What is the Coxeter graph for a free group? For a free Abelian group?

Exercise 1.2. (*) Reverse the braid word $\sigma_1^{-1}\sigma_2\sigma_2^{-1}\sigma_3$ to the right.

Exercise 1.3. (*) Consider the presentation $(a, b; ab = ba^2)$ (Baumslag–Solitar). Reverse the word $a^{-p}b^q$ to the right.

Exercise 1.4. (**) Consider the Artin–Tits presentation with $\Sigma_\Gamma = \{1, 2, 3\}$ and $m_{12} = m_{23} = m_{13} = 3$ (type $\widetilde{A}_2$). Reverse the word $\sigma_1^{-1}\sigma_2\sigma_3$ to the right.

Exercise 1.5. (*) Prove that the presentation $(a, b; aba = bb)$ is homogeneous.

Exercise 1.6. (**) Prove that the presentation $(a, b; ab = baa)$ is homogeneous.

Exercise 1.7. (***) Prove that the presentation $(a, b; ababa = bb)$ is homogeneous.

Exercise 1.8. (*) Prove that every homogeneous presentation with two generators a, b and one relation of the type $av = bu$ is complete for reversing.

Exercise 1.9. (*) Prove that the presentation $(a, b; a^2 = b^2, ab = ba)$ is complete for reversing.

Exercise 1.10. (*) Prove the Lemma 1.3, *i.e.*, check the right of left cube conditions for Artin–Tits presentations.

Exercise 1.11. (**) Show that right reversing the braid word $(\sigma_1\sigma_3\sigma_5\ldots\sigma_{2n-1})^{-1}(\sigma_2\sigma_4\ldots\sigma_{2n})$ requires $\mathcal{O}(n^3)$ steps and finishes with a word of length $\mathcal{O}(n^2)$.

Exercise 1.12. (**) Assume that (Σ, R) is a positive presentation such that, for all σ_i, σ_j in Σ, there is at most one relation $\sigma_i v = \sigma_j u$ in R. For u, v positive Σ-words, let $C(u, v)$ denote the unique positive word v_1 such that $u^{-1}v$ is right R-reversible to $v_1u_1^{-1}$ for some positive u_1, if it exists.

Prove that the presentation is complete for right reversing if and only if C is compatible with R-equivalence, *i.e.*, if u' is equivalent to u and v' is equivalent to v, then $C(u', v')$ is equivalent to $c(u, v)$.

Deduce that every presentation of the type $(a, b; av = bu)$ is complete (the differn ce with Exercise 1.8 is that we do not assume that the presentation is homogeneous).

Exercise 1.13. (**) Prove Lemma 1.4 (cancellativity); extend the statement so as to make it a necessary and sufficient condition.

Exercise 1.14. (**) Assume that (Σ, R) is a positive presentation that is complete for right reversing, and Σ_0 is a subset of Σ. Let R_0 be the set of all relations $\sigma_i v = \sigma_j v$ in R with $\sigma_i, \sigma_j \in \Sigma_0$. Assume that all words occurring in R_0 are Σ_0-words. Show that the submonoid of $\langle \Sigma\,; R\rangle^+$ generated by Σ_0 admits the presentation $\langle \Sigma_0\,; R_0\rangle^+$. Same question for the group, assuming in addition that right reversing always converges.

Exercise 1.15. (***) Assume that reversing solves the word problem of the presentation (Σ, R). Prove that the monoid $\langle \Sigma\,; R\rangle^+$ embeds in the group $(\Sigma; R)$.

2. The spherical case

When $(\mathcal{C})$ is satisfied, one obtains a good control of the Artin–Tits group A_Γ using its connection to A_Γ^+. We aim at connecting the above condition with the associated Coxeter group: when the latter is finite, $(\mathcal{C}^{fin})$ holds, and the Artin–Tits group has a so-called *Garside structure*.

2.1. Background about Coxeter groups.

We borrow without proof two results about Coxeter groups. A word u in Σ_Γ is called *reduced* if no shorter word represents the same element of W_Γ.

Lemma 2.1. *Let Γ be any Coxeter graph.*

(i) *(Exchange Lemma) If u is a reduced word and $\sigma_i u$ is not reduced, there exists a reduced word u' obtained by removing one letter in u such that $\sigma_i u'$ and u represent the same element of W_Γ.*

(ii) *If u, u' are reduced words representing the same element of W_Γ, then one can go from u to u' using the relations of R_Γ exclusively.*

Point (i) is the crucial one; it implies (ii). The combinatorial proofs are rather easy [27].

Corollary 2.2. *Let Γ be any Coxeter graph.*

(i) All reduced expressions of an element x of W_Γ have the same length, henceforth denoted $\ell(x)$.

(ii) For every x, one has $\ell(x\sigma_i) = \ell(x) \pm 1$.

(iii) There exists an element w_0 with maximal length if and only if W_Γ is finite, and, in this case, the element w_0 is unique and, if u is a reduced word, w_0 admits an expression beginning with u, and an expression ending with u.

Proof. (i) The relations of R_Γ preserve the length. Apply Lemma 2.1(ii).

(ii) If u is a reduced expression of x in W_Γ, $u\sigma_i$ is an expression of $x\sigma_i$, so we have $\ell(x\sigma_i) \leqslant \ell(x) + 1$. Applying this to $x\sigma_i^{-1}$, which is also $x\sigma_i$, we obtain $\ell(x) \leqslant \ell(x\sigma_i) + 1$, hence $\ell(x\sigma_i) \geqslant \ell(x) - 1$. Finally $\ell(x\sigma_i) = \ell(x)$ is impossible as the relations presenting W_Γ preserve the parity of the length.

(iii) If W_Γ is has N elements, the relation of (ii) implies that every element has length at most N, so there must exist an element with maximal length.

Conversely, assume that w_0 is an element of maximal length. Let u be any reduced word, say $u = \sigma_{i_1}\ldots\sigma_{i_p}$. We claim that w_0 has a reduced expression beginning with u. To this end, we prove using induction on k descending from p to 0 that w_0 has a reduced expression of the form $\sigma_{i_{k+1}} \dots \sigma_{i_p} u_k$. For $k = p$, we choose u_p to be any reduced expression of w_0. Now, $\sigma_{i_k} \sigma_{i_{i+1}} \dots \sigma_{i_p} u_k$ cannot be reduced, hence, by the Exchange Lemma, there exists a word obtained by removing a letter for $\sigma_{i_{k+1}} \dots \sigma_{i_p} u_k$ that is a reduced expresion of $\sigma_{i_k} w_0$. If the letter is removed from u_k, we call the remaining word uu_{k-1}, and we are done. Now, if the letter is removed from $\sigma_{i_{k+1}} \dots \sigma_{i_p}$, we obtain, by cancelling u_k on the right, that $\sigma_{i_k} \dots \sigma_{i_p}$ is equal to something obtained by removing one letter in $\sigma_{i_k} \dots \sigma_{i_p}$, contradicting the hypothesis that $\sigma_{i_k} \dots \sigma_{i_p}$ is reduced. So the induction goes on. For $k = 0$, we obtain an expression of w_0 that begins with u.

Consider all reduced expressions of w_0. By Lemma 2.1(*ii*), they all are R_Γ-equivalent, hence they all contain the same letters. This implies that only finitely many different letters may occur in reduced expressions of w_0, and, therefore, that there are only finitely mant reduced expressions of w_0. Now we showed above that every reduced word appears in a reduced expression of w_0, hence there are only finitely many such reduced expressions, and, therefore, finitely many elements in W_Γ.

Finally, assume that w_0' is a maximal length element. Then w_0 has a reduced expression u_0 beginning with a reduced expression u_0' of w_0': by maximality of w_0', we have $u_0' = u_0$, hence $w_0' = w_0$. □

Let π denote the canonical surjective morphism of A_Γ onto W_Γ. Lemma 2.1(*ii*) gives a (set-theoretical) section σ to π: for x in W_Γ, define $\sigma(x)$ to be the element of A_Γ represented by any reduced length decomposition of x. By the lemma, the definition is unambiguous.

Lemma 2.3. *Assume that W_Γ is finite and w_0 is the longest element. Let $\Delta = \sigma(w_0)$. Then, for each element x of A_Γ^+, the following are equivalent:*
(i) x belongs to the image of σ; (ii) x is a left divisor of Δ; (iii) x is a right divisor of Δ.

Proof. Assume (i). This means that x has an expression u that is reduced (in the sense of W_Γ). By Corollary 2.2(*iii*), this implies that w_0 has a reduced expression of the form uv. Lifting this by σ, we obtain $\Delta = x\sigma(v)$, which implies (*ii*); the argument for (*iii*) is symmetric.

On the other hand, let S denote the image of σ. We claim that a left divisor of an element x of S still lies in S. Indeed, assume that y is a left divisor of x in A_Γ^+. Then there exists an expression $\sigma_{i_1} \dots \sigma_{i_p}$ of x such that y is $\sigma_{i_1} \dots \sigma_{i_q}$ for some q with $q \leqslant p$. As the relations of R_Γ preserve length, all expressions of x in A_Γ^+ have length p, hence $(\sigma_{i_1}, \dots, \sigma_{i_p})$ is a reduced decomposition of $\pi(x)$ in W_Γ. As multiplying by one σ_i increases the length by 1 at most, an initial subsequence of a reduced decomposition is a reduced decomposition, and y is $\sigma(\pi(y))$, hence lies in S. In particular, any left divisor of Δ belongs to S, *i.e.*, (*ii*) implies (*i*). The argument for right divisors is similar. □

2.2. **Garside structure.** In the 1960's, Garside investigated the braid groups B_n using the monoids B_n^+ [32]. It subsequently appeared that all Garside uses is the existence of what is now called a Garside structure, and that other examples exist, even in the case of braids themselves.

Say that a monoid is an *lcm monoid* if any two elements admit a left and a right lcm. Provided no element has an infinite chain of divisors (as is the case with every Artin–Tits monoid), the existence of lcm's implies that of gcd's.

Definition. (*i*) An element Δ of a monoid M is called a *Garside element* if the left and right divisors of Δ coincide, they generate M, and they are finite in number.

(*ii*) A *Garside monoid* is a pair (M, Δ) where M is a cancellative monoid in which any two elements of M admit a left and a right lcm, and Δ is a Garside element in M.

(*iii*) Let G be a group. A *Garside structure* for G is a Garside monoid (M, Δ) such that M is a submonoid of G and G is a group of left and right fractions of M.

Note that the hypothesis that M is a submonoid of G implies that M is cancellative, and the hypothesis that G is a grou pof fractions of M implies that any two elements of M admit common left and right multiples (but not necessarily lcm's).

Proposition 2.4. *Assume that Γ is a Coxeter graph such that W_Γ is finite. Let Δ be the lifting of the longest element of W_Γ in A_Γ^+. Then $(\mathrm{A}_\Gamma^+, \Delta)$ is a Garside structure for the Artin–Tits group A_Γ.*

Proof. First Δ is a Garside element in A_Γ^+. Indeed, each generator σ_i belongs to the image of s, hence, by Lemma 2.3, it divides Δ, so the divisors of Δ generate A_Γ^+. On the other hand, Lemma 2.3 says that the left and right divisors of Δ coincide. Finally, the divisors of Δ are in one-to-one correspondence with the elements of W_Γ, hence they are finite in number. Hence Δ is a Garside element in A_Γ^+.

Let S be the set of (left and right) divisors of Δ. Any two elements of S admit a common right multiple, namely Δ. Hence $(\mathcal{C}^{fin})$ holds. By the results of Section 1, the monoid A_Γ^+ is cancellative, and any two elements admit a left and a right lcm. Hence A_Γ is a group of (left and right) fractions of A_Γ^+. □

2.3. **Normal form.** The existence of a Garside structure on a group gives lots of information about that group; in the case of Artin groups associated with finite Coxeter groups, a large amount of the known results follow from the Garside structure. We establish a few results involving in particular the construction of unique normal forms. We denote by $x \wedge y$ the left gcd of x and y.

Proposition 2.5. *(i) Assume that (M, Δ) is a Garside structure for G. Then every element of G admits a unique expression $x^{-1}y$ with x, y in M and $x \wedge y = 1$.*

(ii) If (Σ, R) is a presentation of M that is complete for reversing, the irreducible decomposition of the element represented by a word w is obtained by double reversing from w: transform w into vu^{-1} using right reversing, then vu^{-1} into $u'^{-1}v'$ using left reversing; then u' (resp. v') represents x (resp. y).

Proof. (i) Uniqueness: assume $x^{-1}y = x'^{-1}y'$. Choose z, z' satisfying $zx = z'x'$. Then one has $zy = zxx^{-1}y = z'x'x'^{-1}y' = z'y'$. The assumption $x \wedge y = 1$ implies $zx \wedge zy = z$, and, similarly, $x' \wedge y' = 1$ implies $z'x' \wedge z'y' = z'$, hence $z = zx \wedge zy = z'x' \wedge z'y' = z' = z'$, then $x = x'$ and $y = y'$.

(ii) First w, vu^{-1} and $u'^{-1}v'$ represent the same element of G. By construction, $u'v$ and $v'u$ represent the left lcm of the elements represented by v and u, hence they have no common left divisor but 1. □

So, now, it suffices to look for normal forms in a Garside monoid. For (M, Δ) a Garside monoid, the divisors of Δ are called *simple*. Now comes the main property. For x, y in a Garside monoid (M, Δ), say that $x \supseteq y$ holds if every simple left divisor of xy is a left divisor of y.

Lemma 2.6. *Let (M, Δ) be a Garside monoid. Then $x \supseteq y \supseteq z$ implies $x \supseteq yz$.*

Proof. Let s a simple left divisor of xyz. Let $x = x_1 \cdots x_p$ be a decomposition of x as a product of simple elements. Let $x_1 s_1 = x_1 \vee s$, and, inductively, let $x_k s_k = x_k \vee s_{k-1}$. Then, inductively, each s_k is simple. The hypothesis that s divides xyz, *i.e.*, $x_1 \ldots x_p yz$, implies that s_k divides yz. The hypothesis $y \supseteq z$ implies that s_p divides y. Hence, coming back, this implies that s divides xy, and the hypothesis $x \supseteq y$ then implies that s' divides x. □

Proposition 2.7. *(i) Let (M, Δ) be a Garside monoid. Then every element of M admits a unique decomposition $x_1 \ldots x_p$ with $x_1, \ldots, x_p$ simple and $x_k \supseteq x_{k+1}$ for every k.*

(ii) If $x_1 \ldots x_p$ is the normal decomposition of x and s is a simple right divisor of x, then the normal decomposition of xs^{-1} is $x'_1 \ldots x'_p$, with $s_{p+1} = s$ and $x'_k s_{k+1} = s_k x_k = x_k \vee_{left} s_{k+1}$.

(iii) If $x_1 \ldots x_p$ is the normal decomposition of x, then the normal decomposition of $x\Delta$ is $\Delta x'_1 \ldots x'_p$, with $x'_k = \Delta^{-1} x_k \Delta$ for each k.

(iv) If (Σ, R) is a presentation of M that is complete for reversing, and $(u_1, \ldots, u_p)$ is a normal decomposition of an element x, i.e., for each k, the word u_k represents the simple element that is the kth factor of the normal decomposition of x, then, for every simple element s and every expression v of s, the normal decomposition of xs^{-1} is obtained by reversing $u_1 \ldots u_p v^{-1}$ to the left.

Proof. (i) First, every element x of M admits a maximal simple divisor, namely $x \wedge \Delta$. Starting with x, let $s_1 = x \wedge \Delta$, and, inductively, let $\sigma_k = (s_{k-1}^{-1} \ldots s_1^{-1} x) \wedge \Delta$. If x divides Δ^e, the process must stop after e steps at most. Then $s_k \supseteq s_{k+1} \ldots s_p$ holds for every k, hence so does $s_k \supseteq s_{k+1}$ *a fortiori*.

Conversely, assume that $s_1 \ldots s_p$ is a decomposition satisfying the hypotheses of the proposition. Then, by Lemma 2.6, we have $s_k \supseteq s_{k+1} \ldots s_p$, so s_k is the maximal simple divisor of $s_k \ldots s_p$ for each k, and the decomposition is the one above.

(ii) The hypothesis that s is a right divisor of x guarantees that $s_0 = 1$, so $x'_1 \ldots x'_p$ is a decomposition of xs^{-1}. The point is to prove that the sequence $(x'_1, \ldots, x'_p)$ is normal, *i.e.*, that $x'_k \supseteq x'_{k+1}$ holds for each k. Assume that s' is a simple left divisor of $x'_k x'_{k+1}$. Then s' is a left divisor of $x'_k x'_{k+1} s_{k+1}$, which is $s_k x_k x_{k+1}$. Let $s_k s'' = s' \vee s_k$. Then the hypothesis that s' divides $s_k x_k x_{k+1}$ implies that s'' divides $x_k x_{k+1}$, so $x_k \supseteq x_{k+1}$ implies that s'' divides x_k, and, therefore, s' divides $s_k x_k$, which is $x'_k s_{k+1}$. So s' is a left divisor of $x'_k x'_{k+1} \vee_{left} x'_k s_{k+1}$, which is x'_k as x'_{k+1} and s_{k+1} are left co-prime by hypothesis. Hence $x'_k \supseteq x'_{k+1}$.

(iii) is left as an exercise (use Exercise 2.9 below); (iv) is a direct translation of (ii). □

The Garside structure arising on the group A_Γ in connection with the monoid A_Γ^+ is not the only possible Garside structure. It was recently shown that alternative Garside structures exist: see [10] for the braid groups, and [7, 6] for some other Artin–Tits groups associated with finite Coxeter groups. Very recently, quasi-Garside structures (a variant in which one does not require that the divisors of the Garside element be finite in number) have been found on some Artin–Tits groups associated with infinite Coxeter groups, firstly the free groups [5] and, conjecturally, all Artin–Tits groups (N. Brady, J. Crisp, A. Kaul, J. McCammond).

2.4. **Exercises.**

Exercise 2.1. (*) What is the normal form in the case of a free Abelian group? Write the normal form of $a^{-2}bcb^{-1}aca^2b^3$.

Exercise 2.2. (*) Draw the restriction of the Cayley graph of A_Γ^+ to the divisors of Δ when A_Γ^+ is a free Abelian monoid of rank 3, or the braid monoid B_3^+, or the braid monoid B_4^+.

Exercise 2.3. (*i*) (**) Assume that (M, Δ) is a Garside structure for a group G. Show that every element of M has finitely many divisors only. Deduce that there exists a mapping $\lambda : M \to \mathbf{N}$ such that $x \neq 1$ implies $\lambda(x) \geqslant 1$ and $\lambda(xy) \geqslant \lambda(x) + \lambda(y)$.

(*ii*) (***) Assume that Σ is a set of divisors of Δ that generates M (for instance, the set of all divisors of Δ). For σ_i, σ_j in Σ, choose two words u, v in Σ such that $\sigma_i v$ and $\sigma_j v$ represent the right lcm of x and y. Let R be the set of all relations $\sigma_i v = \sigma_j u$ arising in this way. Show that (Σ, R) is a presentation of M and of G that is complete for right reversing. [Hint: Show that u, v representing the same element of M implies u, v R-equivalent using induction on $\lambda(u)$.]

Exercise 2.4. (**) Prove the Exchange Lemma for a free Abelian group, and for a symmetric group.

Exercise 2.5. (**) Let M be the submonoid of B_3 generated by $a = \sigma_1$ and $b = \sigma_2\sigma_1$, and let $\Delta = b^3$. Show that (M, Δ) is a Garside structure for B_3.

Exercise 2.6. (**) Let M be the submonoid of B_3 generated by $a = \sigma_1$, $b = \sigma_2$ and $c = \sigma_2^{-1}\sigma_1\sigma_2$, and let $\Delta = ab$. Show that (M, Δ) is a Garside structure for B_3 (one more!).

Exercise 2.7. (**) Assume that (M, Δ) is a Garside structure for G. Show that (M, Δ^e) is also a Garside structure for G for $e \geqslant 1$.

Exercise 2.8. (*i*) (**) Let M be a cancellative lcm monoid. For x, y in M, denote by $x \vee y$ the right lcm of x and y, and by $x\backslash y$ the unique z satisfying $x \vee y = xz$. Prove

$$(xy)\backslash z = y\backslash(x\backslash z), \qquad z\backslash(xy) = (z\backslash x)\cdot((x\backslash z)\backslash y)$$
$$(x \vee y)\backslash z = (x\backslash y)\backslash(x\backslash z) = (y\backslash x)\backslash(y\backslash z), \qquad z\backslash(x \vee y) = (z\backslash x) \vee (z\backslash y)$$

(*ii*) (***) Under the same hypotheses, show that $x_1x_2 = y_1y_2$ is equivalent to

$$x_2\backslash(x_1\backslash y_1) = 1, \quad ((x_1\backslash y_1)\backslash x_2)\backslash((y_1\backslash x_1)\backslash y_2) = 1,$$
$$y_2\backslash(y_1\backslash x_1) = 1, \quad ((y_1\backslash x_1)\backslash y_2)\backslash((x_1\backslash y_1)\backslash x_2) = 1.$$

By extending this example, prove that, if Σ is a generating subset of M that is closed under $\backslash$, then the monoid structure of M is fully determined by the restriction of $\backslash$ to Σ. Apply this to show that, if (M, Δ) is a Garside structure for a group G, then G is fully determined by the restriction of $\backslash$ to the divisors of Δ in M.

Exercise 2.9. (**) Assume that (M, Δ) is a Garside structure for G. Show that conjugation by Δ induces an automorphism ϕ of M. Prove that ϕ has finite order, and deduce that some power of Δ belongs to the centre of G.

Exercise 2.10. (***) Assume that G is the group of fractions of a monoid M with any two elements admit a right lcm. Prove that every torsion element of M can be expressed as xtx^{-1} with x in M and t a torsion element of M. Deduce that Artin–Tits group of spherical type have no torsion.

Exercise 2.11. (***) Prove that the normal form given by Propositions 2.5 and 2.7 gives rise to an automatic structure, *i.e.*, the set of normal words can be decided by a finite state automaton and the Fellow Traveler Property holds: there exists a constant C such that, if u, v are normal words representing elements of the group that differ by one generator, then the distance between the paths specified by u and v in the Cayley graph are uniformly bounded by C.

3. The braid case

The Artin–Tits groups of type A_n, *i.e.*, the braid groups, have additional properties not shared by the other groups of the family. Here we describe an explicit ordering with a very simple combinatorial characterization. The braid ordering has many equivalent constructions, and many properties [25]. Here we try to give the shortest possible access. In the sequel, the following braid words will play a crucial role.

Definition. We say that a braid word is σ_i*-positive* if it contains at least one letter σ_i, but no σ_i^{-1} or $\sigma_j^{\pm 1}$ with $j < i$. We say that a braid is σ-positive if, among its various expressions by braid words, there is at least one that is σ_i-positive for some i.

3.1. **The Artin representation.** The Artin representation of B_n into the automorphisms of a free group is important in itself, so it is interesting to mention it independently of its subsequent use for constructing the braid ordering.

The very elegant construction relies on a topological approach, and we shall be sketchy. However, as topology is used here for guessing the explicit formulas only, the subsequent proof that one obtains a faithful representation of B_n will be complete.

The starting point is to identify the braid group B_n with the group of homotopy classes of self-homeomorphisms of an n-punctured disk. The idea is simply to look at braids from one end rather than from the side. Let D^2 be a disk. We denote by D_n the pair (D^2, P_n), where P_n is a set of n points in the interior of D^2 (punctures). The *mapping class group* $MCG(D_n)$ is defined to be the group of all isotopy classes of orientation-preserving homeomorphisms $\varphi : D^2 \to D^2$ that fixe the boundary pointwise and map P_n to itself. Note that the punctures may be permuted by φ. Two homeomorphisms φ, ψ represent the same element if and only if they are isotopic through a family of boundary-fixing homeomorphisms which also fix P_n. The group structure on $MCG(D_n)$ is given by composition.

Proposition 3.1. *The groups B_n and $MCG(D_n)$ are isomorphic.*

Proof. Let β be a geometric n-braid, sitting in the cylinder $[0,1] \times D^2$, whose n strands are starting at the puncture points of $\{0\} \times D_n$ and ending at the puncture points of $\{1\} \times D_n$. The braid may be considered as the graph of the motion, as time goes from 1 to 0, of n points moving in the disk, starting and ending at the puncture points (letting time go from 0 to 1 would lead to an anti-isomorphism). It can be proved that this motion extends to a continuous family of homeomorphisms of the disk, starting with the identity and fixed on the boundary at all times. The end map of this isotopy is the corresponding homeomorphism $\varphi : D_n \to D_n$, which is well-defined up to isotopy fixed on the punctures and the boundary.

Conversely, given a homeomorphism $\varphi : D_n \to D_n$, representing some element of the mapping class group, we want to get a geometric n-braid. By a well-known trick of Alexander, any homeomorphism of a disk which fixes the boundary is isotopic to the identity, through homeomorphisms fixing the boundary. The corresponding braid is the graph of the restriction of such an isotopy to the puncture points. □

An homeomorphism of D_n takes loops in D_n to themselves, and it therefore induces an automorphism of its fundamental group. The latter is a free group of rank n: for each puncture, we fix a loop that makes one turn around that puncture. By reading Figure 4, we obtain a homomorphism of B_n into the automorphism of the free group of rank n, denoted F_n:

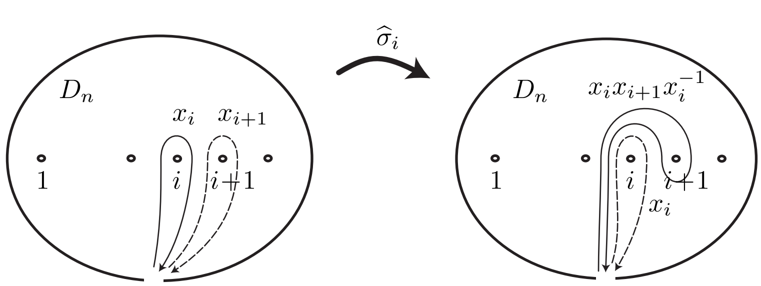


Figure 4. Artin representation of B_n: action of braids on the generators of the fundamental group of the punctured disk D_n.

Lemma 3.2. *For $1 \leqslant i < n$ let $\widehat{\sigma}_i$ be the automorphism of F_n defined by*

$$\widehat{\sigma}_i: \quad x_i \mapsto x_i x_{i+1} x_i^{-1}, \qquad x_{i+1} \mapsto x_i, \quad x_k \mapsto x_k \quad \text{for } k \neq i, i+1; \tag{3.1}$$

Then mapping σ_i to $\widehat{\sigma}_i$ defines a homomorphism of B_n into $\mathrm{Aut}(F_n)$.

In the sequel, we identify F_n with the set of all freely reduced words on the letters $x_1^{\pm 1}, \dots, x_n^{\pm 1}$; we denote by red the operation of iteratively removing all subowrds xx^{-1} or $x^{-1}x$.

Lemma 3.3. *The image of a reduced word ending with x_i^{-1} under $\widehat{\sigma}_i$ or $\widehat{\sigma}_j^{\pm 1}$ with $j > i$ ends with x_i^{-1}.*

Proof. Assume that u ends with x_i^{-1}, say $u = u' x_i^{-1}$. Then we have

$$\widehat{\sigma}_i(u) = \mathrm{red}(\widehat{\sigma}_i(u') x_i x_{i+1}^{-1} x_i^{-1}). \tag{3.2}$$

In order to prove that the word above ends with x_i^{-1}, it is sufficient to check that the final x_i^{-1} cannot be cancelled during the reduction by some x_i coming from $\widehat{\sigma}_i(u')$. By definition, an x_i in $\widehat{\sigma}_i(u')$ must come from some x_i, x_i^{-1}, or x_{i+1} in u'. We consider the three cases, displaying the supposed involved letter in u'. For $u' = u'' x_i u'''$, (3.2) becomes

$$\widehat{\sigma}_i(u) = \mathrm{red}(\widehat{\sigma}_i(u'') x_i x_{i+1} x_i^{-1} \widehat{\sigma}_1(u''') x_i x_{i+1}^{-1} x_i^{-1}).$$

The assumption that the first x_i cancels the final x_i^{-1} implies $\widehat{\sigma}_i(u''') = \varepsilon$, hence $u''' = \varepsilon$, contradicting the hypothesis that $u'' x_i u''' x_i^{-1}$ is reduced. For $u' = u'' x_i^{-1} u'''$, (3.2) is

$$\widehat{\sigma}_i(u) = \mathrm{red}(\widehat{\sigma}_i(u'') x_i x_{i+1}^{-1} x_i^{-1} \widehat{\sigma}_1(u''') x_i x_{i+1}^{-1} x_i^{-1}).$$

The assumption that the first x_i cancels the final x_i^{-1} implies now that $x_{i+1}^{-1} x_i^{-1} \widehat{\sigma}_i(u''') x_i x_{i+1}^{-1}$ reduces to ε, hence $\widehat{\sigma}_i(u''') = x_i x_{i+1}^2 x_i^{-1}$, and, therefore, $u''' = x_i^2$, again contradicting the hypothesis that $u'' x_i^{-1} u'''$ is reduced. Finally, for $u' = u'' x_{i+1} u'''$, (3.2) says

$$\widehat{\sigma}_i(u) = \mathrm{red}(\widehat{\sigma}_i(u'') x_i \widehat{\sigma}_1(u''') x_i x_{i+1}^{-1} x_i^{-1}).$$

The assumption that the first x_i cancels the final x_i^{-1} implies that $\widehat{\sigma}_i(u''') x_i x_{i+1}^{-1}$ reduces to ε, hence $\widehat{\sigma}_i(u''') = x_{i+1} x_i^{-1}$, and, then, $u''' = x_{i+1}^{-1} x_i$, contradicting the hypothesis that $u'' x_{i+1} u'''$ is reduced. We similarly consider the action of $\widehat{\sigma}_j^e$ with $j > i$ and $e = \pm 1$. We find

$$\widehat{\sigma}_j(u) = \mathrm{red}(\widehat{\sigma}_j^e(u') x_i^{-1}), \tag{3.3}$$

and aim at proving that the final x_i^{-1} cannot vanish in reduction. Now it could do it only with some x_i in $\widehat{\sigma}_j^e(u')$, itself coming from some x_i in u'. For a contradiction, we display the latter as $u' = u'' x_i u'''$. Then (3.3) becomes $\widehat{\sigma}_j(u) = \mathrm{red}(\widehat{\sigma}_j^e(u'') x_i \widehat{\sigma}_j^e(u''') x_i^{-1})$. As above, we must have $\widehat{\sigma}_j^e(u''') = \varepsilon$, hence $u''' = \varepsilon$, contradicting the hypothesis that $u'' x_i u''' x_i^{-1}$ is reduced. □

For w a braid word, we denote by $\widehat{w}$ the automorphism of F_n associated with w.

Proposition 3.4. *Let w be a σ_i-positive braid word. Then the automorphism $\widehat{w}$ is not trivial.*

Proof. Write $w = w_0 \sigma_i w_1 \sigma_i \dots \sigma_i w_r$, where w_k contains no $\sigma_j^{\pm 1}$ with $j \leqslant i$. Then $\widehat{w_r}$ fixes x_i, while σ_i maps it to $x_i x_{i+1} x_i^{-1}$, a reduced word ending with x_i^{-1}. Applying Lemma 3.3 repeatedly, we deduce that the final x_i^{-1} cannot disappear, and, so, $\widehat{w}(x_i)$ is a reduced word ending with x_i^{-1}. Hence $\widehat{w}$ cannot be the identity mapping. □

Corollary 3.5. *A σ-positive braid is not trivial (i.e., equal to 1).*

3.2. Handle reduction.

Our aim isnow to prove

Proposition 3.6. *Every non-trivial braid is either σ-positive or σ-negative.*

In the above statement, a σ-negative braid is one whose inverse is σ-positive. As σ-positive braids are clearly closed under multiplication, Corollary 3.5 implies that a braid cannot be simultaneously σ-positive and σ-negative, as this would imply that 1 is σ-positive.

We shall not only prove Proposition 3.6, but also describe an algorithmic process that, starting with an arbitrary braid word w, returns an equivalent braid word that is either σ-positive, or σ-negative, or empty. The idea of the method is simple. Assume that w is a nonempty braid word that is neither σ-positive nor σ-negative: this means that, if i is the smallest index such that $\sigma_i^{\pm 1}$ appears in w, then both σ_i and σ_i^{-1} appear in w. So, necessarily, w contains some subword of the form $\sigma_i^e \partial^i(u) \sigma_i^{-e}$ with $e = \pm 1$, where ∂ denotes the word homomorphism that maps every letter $\sigma_i^{\pm 1}$ to $\sigma_{i+1}^{\pm 1}$—as well as the induced endomorphism of B_∞.

Definition. A braid word of the form $\sigma_i^e \partial^i(u) \sigma_i^{-e}$ with $e = \pm 1$ is called a *σ_i-handle.*

Thus, every braid word that is neither σ-positive nor σ-negative must contain a σ_i-handle. We can get rid of a handle by pushing the strand involved in the handleas shown in Figure 5(left). We call this transformation *reduction* of the handle. We can then iterate handle reduction until no handle is left: if the process converges, then, by construction, the final word contains no handle, which implies that it is either σ-positive, or σ-negative, or empty. This naive approach does not work readily: when applied to the word $w = \sigma_1\sigma_2\sigma_3\sigma_2^{-1}\sigma_1^{-1}$, it leads in one step to the word $w' = \sigma_2^{-1} w \sigma_2$: the initial handle is still there, and iterating the process leads to nothing but longer and longer words. Now, the handle in w' is not the original handle of w, but it comes from the σ_2-handle $\sigma_2\sigma_3\sigma_2^{-1}$ of w. If we reduce the latter handle into $\sigma_3^{-1}\sigma_2\sigma_3$ before reducing the main handle of w, *i.e.*, if we first go from w to $w'' = \sigma_1\sigma_3^{-1}\sigma_2\sigma_3\sigma_1^{-1}$, then applying handle reduction yields $\sigma_3^{-1}\sigma_2^{-1}\sigma_1\sigma_2\sigma_3$, a σ-positive word equivalent to w.

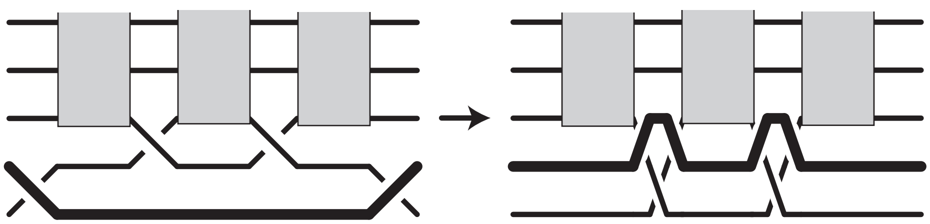


FIGURE 5. A permitted handle (left), and its reduction (right)

Definition. A handle $\sigma_i^e v \sigma_i^{-e}$ is said to be *permitted* if the word v includes no σ_{i+1}-handle. We say that the braid word w' is obtained from the braid word w *by a one-step handle reduction* if some subword of w is a permitted σ_i-handle, say $\sigma_i^e v \sigma_i^{-e}$, and w' is obtained from w by applying in the latter handle the alphabetical homomorphism

$$\sigma_i^{\pm 1} \mapsto \varepsilon, \quad \sigma_{i+1}^{\pm 1} \mapsto \sigma_{i+1}^{-e}\sigma_i^{\pm 1}\sigma_{i+1}^{e}, \quad \sigma_k^{\pm 1} \mapsto \sigma_k^{\pm 1} \text{ for } k \geqslant i+2.$$

The general form of a σ_i-handle is

$$\sigma_i^e \, v_0 \, \sigma_{i+1}^{d_1} \, v_1 \, \sigma_{i+1}^{d_2} \ldots \sigma_{i+1}^{d_k} \, v_k \, \sigma_i^{-e}$$

with $d_j = \pm 1$ and $v_j \in \partial^{i+1}(B_\infty)$. Saying that this handle is permitted amounts to saying that all exponents d_j have a common value d. Then, reducing the handle means replacing it with

$$v_0 \, \sigma_{i+1}^{-e}\sigma_i^d\sigma_{i+1}^e \, v_1 \, \sigma_{i+1}^{-e}\sigma_i^d\sigma_{i+1}^e \ldots \sigma_{i+1}^{-e}\sigma_i^d\sigma_{i+1}^e \, v_k :$$

we remove the initial and final $\sigma_i^{\pm 1}$, and replace each σ_{i+1}^d with $\sigma_{i+1}^{-e}\sigma_i^d\sigma_{i+1}^e$.

Lemma 3.7. *Handle reduction transforms a word into an equivalent word. If a nonempty braid word w is terminal w.r.t. handle reduction, i.e., if w contains no handle, then w is σ-positive or σ-negative.*

Observe that handle reduction generalizes free reduction: $\sigma_i\sigma_i^{-1}$ and $\sigma_i^{-1}\sigma_i$ are particular σ_i-handles, and reducing them amounts to deleting them.

Definition. We say that a nonempty braid word w has *width n* if the difference between the smallest and the largest indices i such that σ_i or σ_i^{-1} occurs in w is $n-2$.

The width of w is the size of the smallest interval containing the indices of all strands really braided in w. So, every n-strand braid word has width at most n, but the inequality may be strict: for instance, the 8-strand braid word $\sigma_3\sigma_7^{-1}$ has width 6.

We shall prove:

Proposition 3.8. *Let w be a braid word of length ℓ and width n. Then every sequence of handle reductions from w converges in at most $2^{n^4\ell}$ steps.*

Clearly, Proposition 3.8 implies Proposition 3.6.

Handle reduction may increase the length of the braid word it is applied to. Our first task for proving convergence of handle reduction will be to show that all words obtained w using handle reduction remain traced in some finite region of the Cayley graph of B_∞ depending on w . To this end, we connect the operation of handle reduction with the operations of left and right reversing defined in Section 1.

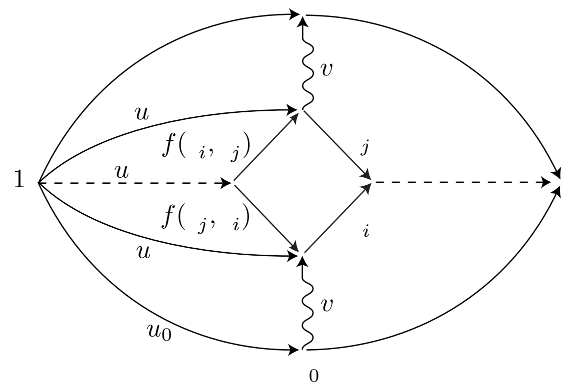


Figure 6. Closure of words traced under left reversing

For every braid word w, we denote by $N_L(w)$ and $D_L(w)$ the unique positive words such that w is left reversible to $D_L(w)^{-1}N_L(w)$, and, symmetrically, by $N_R(w)$ and $DR(w)$ the positive words such that w is right reversible to $N_R(w)D_R(w)^{-1}$.

The general notion of the Cayley graph of a group (with respect to specified generators) is well-known. Here we consider finite fragments of such graphs.

Definition. Assume that β is a positive braid. The *Cayley graph of* β is the finite labelled oriented graph $\Gamma(\beta)$ defined as follows: the vertices are the left divisors of β, and there exists an edge labelled σ_i from the vertex β_1 to the vertex β_2 if $\beta_2 = \beta_1\sigma_i$ holds.

When we are given a graph Γ whose (oriented) edges are labelled using letters from some alphabet A, we have the natural notion of a word *traced* in Γ: for w a word on the alphabet A, we say that w is traced in Γ from the vertex β_0 if there exists in Γ a path starting at β_0 labelled w, *i.e.*, w is the word obtained by concatenating the labels of the edges in that path, with exponents ± 1 according as the edge orientation agrees or disagrees with that of the path. For our current purpose, the point is that, for every positive braid β, the set of all words traced in the Cayley graph of β enjoys good closure properties.

Lemma 3.9. *Assume that β is a positive braid. Then the set of all words traced in $\Gamma(\beta)$ from a given point is closed under left and right reversing.*

Proof. Let us consider left reversing. So we assume that some word $v\,\sigma_i\,\sigma_j^{-1}\,v'$ is traced from β_0 in $\Gamma(\beta)$, and we have to show that $v\ f(\sigma_j,\sigma_i)^{-1}\ f(\sigma_i,\sigma_j)\ v'$ is also traced from β_0 in $\Gamma(\beta)$. Let u_0 be a positive word representing β_0. The hypothesis means that there exist positive braid words u, u' such that both $u\sigma_i$ and $u'\sigma_j$ are traced from 1 in $\Gamma(\beta)$, the equivalence $u\sigma_i \equiv u'\sigma_j$ is satisfied, and, moreover, we have $u \equiv u_0 v$ (Figure 6). Right lcm's exist in B_∞^+, hence $u\sigma_i \equiv u'\sigma_j$ implies that there exists a positive braid word u'' satisfying $u \equiv u'' f(\sigma_j,\sigma_i)$ and $u' \equiv u'' f(\sigma_i,\sigma_j)$. By definition of the Cayley graph of β, the words $u'' f(\sigma_j,\sigma_i)\sigma_i$ and $u'' f(\sigma_i,\sigma_j)\sigma_j$ are traced in $\Gamma(\beta)$, since they are both equivalent to $u\sigma_i$. This shows that the edges $f(\sigma_j,\sigma_i)^{-1}$ and $f(\sigma_i,\sigma_j)$ needed to complete the path labelled $vf(\sigma_j,\sigma_i)^{-1}f(\sigma_i,\sigma_j)v'$ from β_0 are in $\Gamma(\beta)$, as was expected. The argument is symmetric for right reversing. □

Say that two (not necessarily positive) braid words w, w' are *positively* (*resp. negatively*) equivalent if one can transform w into w' using the positive braid relations (*resp.* the inversed braid relations).

Lemma 3.10. *Assume that β is a positive braid. Then the set of all words traced in $\Gamma(\beta)$ from a given point is closed under positive and negative equivalence.*

Proof. Assume, for instance, that $v\sigma_i\sigma_{i+1}\sigma_i v'$ is traced in $\Gamma(\beta)$ from β_0. Let u_0 be a positive word representing β_0. Now v is not necessarily a positive word, but, by definition, there exists a positive word u such that $u\sigma_i\sigma_{i+1}\sigma_i$ is traced in $\Gamma(\beta)$ from 1 and $u_0 v \equiv u$ holds. Now $u\sigma_{i+1}\sigma_i\sigma_{i+1}$ is a positive word equivalent to $u\sigma_i\sigma_{i+1}\sigma_i$, so it is traced from 1 in $\Gamma(\beta)$, and, therefore, $v\sigma_{i+1}\sigma_i\sigma_{i+1}v'$ is still traced in $\Gamma(\beta)$ from β_0. The case of negative equivalence is similar and corresponds to traversing the edges with reversed orientation. □

If w is a braid word, we use $\overline{w}$ for the braid represented by w. The following result gives a sort of upper bound for the words that can be deduced from a given braid word using reversing and signed equivalence, *i.e.*, essentially, when introducing new patterns $\sigma_i\sigma_i^{-1}$ or $\sigma_i^{-1}\sigma_i$ is forbiden.

Proposition 3.11. *Assume that w is a braid word. Denote by $|w|$ the positive braid represented by the (equivalent) words $D_L(w)N_R(w)$ and $N_L(w)D_R(w)$. Then every word obtained from w using left reversing, right reversing, positive equivalence, and negative equivalence is traced from $\overline{D_L(w)}$ in $\Gamma(|w|)$.*

Owing to Lemmas 3.9 and 3.10, it only remains to show that w itself is traced from $\overline{D(w)}$ in $\Gamma(|w|)$. The verification is an easy exercise.

If w' is obtained from w using handle reduction, then w' is equivalent to w. This obvious fact can be refined into the following result.

Lemma 3.12. *Assume that w' is obtained from w using handle reduction. Then one can transform w into w' using right reversing, left reversing, positive equivalence, and negative equivalence.*

Proof. The point is to show that, for $v_0, \ldots, v_k$ in $\partial^{i+1}(B_\infty)$, we can go from

$$\sigma_i^e\, v_0\, \sigma_{i+1}^d\, v_1\, \sigma_{i+1}^d\, \ldots\, \sigma_{i+1}^d\, v_k\, \sigma_i^{-e} \tag{3.4}$$

to

$$v_0\, \sigma_{i+1}^{-e}\sigma_i^d\sigma_{i+1}^e\, v_1\, \sigma_{i+1}^{-e}\sigma_i^d\sigma_{i+1}^e\, \ldots\, \sigma_{i+1}^{-e}\sigma_i^d\sigma_{i+1}^e\, v_k : \tag{3.5}$$

using the transformations mentioned in the statement. Assume for instance $e = +1$ and $d = -1$. Then reduction can be done by moving the initial σ_i to the right. First transforming $\sigma_i v_0$ into $v_0\sigma_i$ can be made by a sequence of left reversings (in the case of negative letters) and positive equivalences (in the case of positive letters). Then we find the pattern $\sigma_i\sigma_{i+1}^{-1}$, which becomes $\sigma_{i+1}^{-1}\sigma_i^{-1}\sigma_{i+1}\sigma_i$ by a left reversing. So, at this point, we have transformed the initial word into

$$v_0\ \sigma_{i+1}^{-1}\sigma_i^{-1}\sigma_{i+1}\sigma_i\ v_1\ \sigma_{i+1}^{-1}\ v_2\ \ldots\ v_{k-1}\ \sigma_{i+1}^{-1}\ v_k\ \sigma_i^{-1}. \tag{3.6}$$

After k such sequences of reductions, and a last left reversing to delete the final pattern $\sigma_i\sigma_i^{-1}$, we reach the form (3.5), as we wished. The argument is similar in the case $e = -1$, $d = 1$, with negative equivalences instead of positive equivalences, and right reversing instead of left reversing. In the case when the exponents e and d have the same sign, we use a similar procedure to move the final generator σ_i^{-e} to the left. □

By applying Proposition 3.11, we deduce:

Proposition 3.13. *Assume that the braid word w' is obtained from w using handle reduction. Then w' is traced in the Cayley graph of $|w|$ from $\overline{D(w)}$.*

The previous result is not sufficient for proving that handle reduction converges. In particular, it does not discard the possibility that loops occur. To go further, we need a new parameter.

Definition. Assume that w is a braid word. The *height* of w is defined to be the maximal number, over all i, of letters σ_i occurring in σ_i-positive word traced in the Cayley graph of $|w|$.

Lemma 3.14. *Let w be a braid word of length ℓ and width n. Then the height of w is bounded above by $(n-1)^{\ell n(n-1)/2}$.*

Proof. Assume that u is a σ_i-positive word traced in $\Gamma(|w|)$. By Corollary 3.5, the edges σ_i involved in the path associated with u must be pairwise distinct. So an upper bound on the number of σ_i in u is the total number of σ_i's in $\Gamma(|w|)$. The latter can be roughly bounded by the given value. □

Let us now consider handle reduction. Assume that $w_0 = w$, $w_1, \ldots$ is a sequence of handle reductions from w. The first point is that the number of σ_1-handles in w_i is not larger than the number of σ_1-handles in w, as reducing one σ_1-handle lets at most one new σ_1-handle appear. We deduce a well-defined notion of inheriting between σ_1-handles such that each σ_1-handle in the initial word w possesses at most one heir in each word w_k. We shall assume that the number of σ_1-handles in every word w_k is the same as in w_0. If it is not the case, *i.e.*, if some σ_1-handle vanishes without heir, say from w_k to w_{k+1}, we cut the sequence at w_k and restart from w_{k+1}. In this way, the heir of the pth σ_1-handle of w_0 (when enumerated from the left) is the pth σ_1-handle of w_k. Let us define the pth *critical prefix* $\pi_p(w_k)$ of w_k to be the braid represented by the prefix of w_k ending at the first letter of the pth σ_1-handle. There are two cases

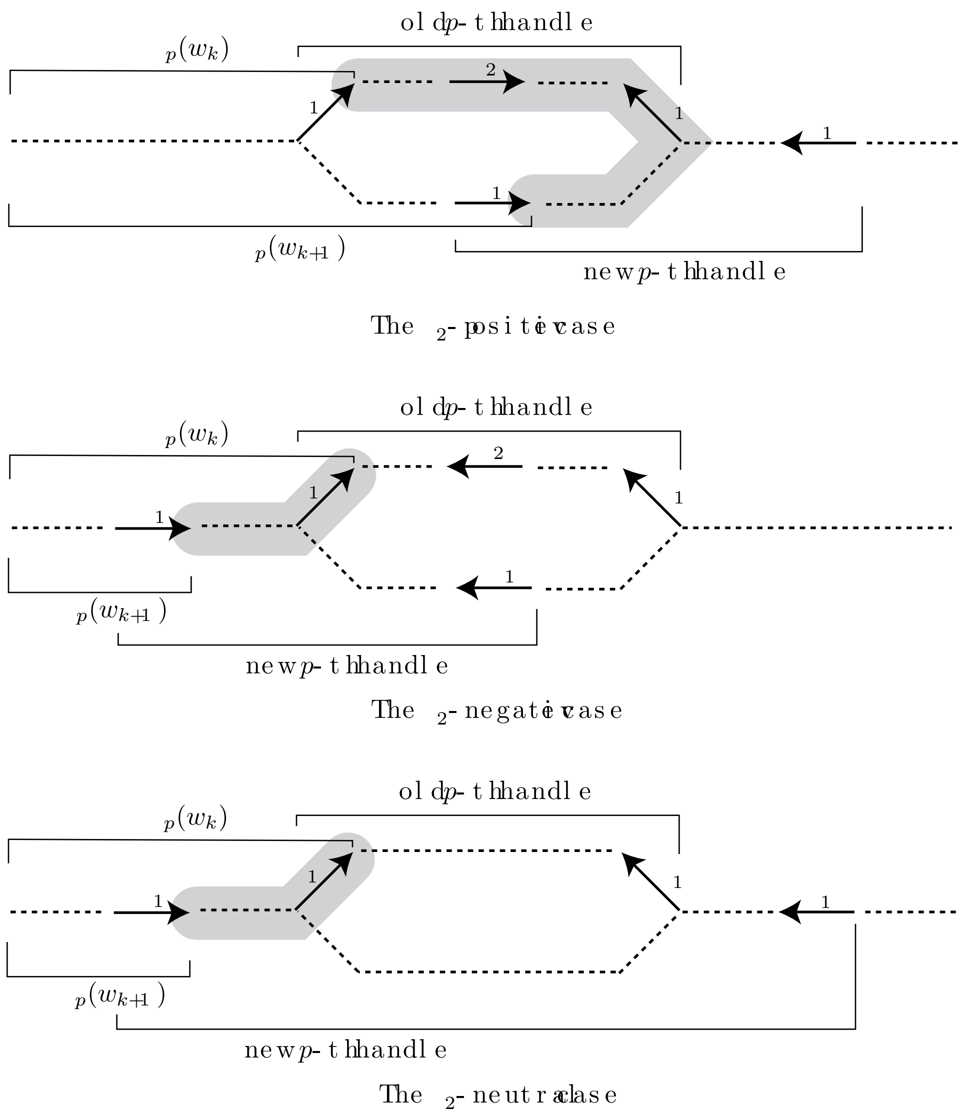


FIGURE 7. Critical prefixes

according to whether the first letter of the handle is σ_1 or σ_1^{-1}. We shall assume here that this letter is σ_1, and briefly mention at the end of the argument the changes for the σ_1^{-1}-case.

The key point is the following observation:

Lemma 3.15. *Assume that the pth σ_1-handle is reduced from w_k to w_{k+1}, and that the handle begins with σ_1^{+1}. Then some braid word $u_{p,k}$ traced in $\Gamma(|w|)$ from $\pi_p(w_k)$ to $\pi_p(w_{k+1})$ contains one σ_1^{-1} and no σ_1.*

Proof. The result can be read on the diagrams of Figure 7, where we have represented the paths associated respectively with w_k (up) and w_{k+1} (down) in the Cayley graph of B_∞, assuming that the pth σ_1-handle has been reduced. The word $u_{p,k}$ appears in grey, and the point is that, in every case, *i.e.*, both if σ_2 appears positively or negatively (or not at all) in the handle, this word $u_{p,k}$ contains one letter σ_1^{-1} and no letter σ_1. □

If the handle reduction from w_k to w_{k+1} is not the pth σ_1-handle, several cases are possible. If the reduction involves a σ_i-handle with $i \geqslant 2$, or it involves the qth σ_1-handle with $q \neq p \pm 1$, then we have $\pi_p(w_k) \equiv \pi_p(w_{k+1})$, and we complete the definition with $u_{p,k} = \varepsilon$. If the reduction involves the $p \pm 1$st σ_1-handle, the equivalence $\pi_p(w_k) \equiv \pi_p(w_{k+1})$ need not be true in general, but, as can be seen on Figure 7 again, some word $u_{p,k}$ containing neither σ_1 nor σ_1^{-1} goes from $\pi_p(w_k)$ to $\pi_p(w_{k+1})$ in $\Gamma(|w|)$. Now, by

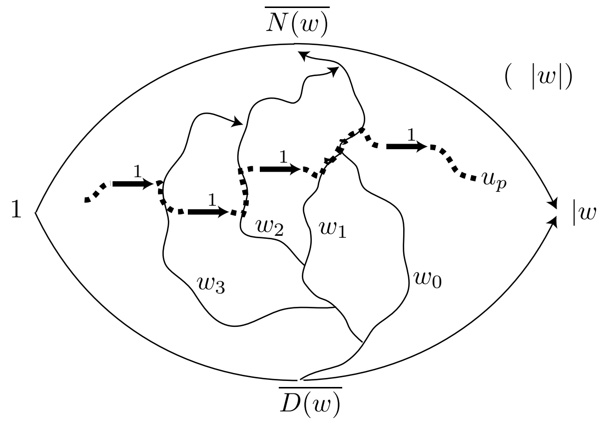


FIGURE 8. Upper bound on the number of σ_1-handle reductions: the witness word u_p contains one letter σ_1 for each reduction of the pth σ_1-handle—and no letter σ_1^{-1}.

construction, the word $u_p = u_{p,0}u_{p,1}u_{p,2}\dots$ is traced in the Cayley graph of $|w|$, it is σ_1-negative, and the number N of steps in the sequence $(w_0, w_1, \dots)$ where the pth σ_1-handle has been reduced is equal to the number of letters σ_1^{-1} in u (see Figure 8). It follows that the number N is bounded above by the height of w, say h. In the case of a pth handle beginning with σ_1^{-1}, the argument is similar, with σ_1 and σ_1^{-1} exchanged in Lemma 3.15.

Finally, in every case, the heirs of each σ_1-handle of the initial word w are involved in at most h reduction steps, and we can state:

Lemma 3.16. *Assume that w is a braid word of height h containing c σ_1-handles. Then the number of σ_1-handle reductions in any sequence of handle reductions from w is bounded above by ch.*

Assuming again that $w_0 = w, w_1, \dots$ is a sequence of handle reductions from w, we can now iterate the result and consider the σ_2-handle reductions: the previous argument gives an upper bound for the number of σ_2-handle reductions between two successive σ_1-handle reductions, and, more generally, for the number of σ_{i+1}-handle reductions between two σ_i-handle reductions. Using a coarse upper bound on the lengths of the words w_i, one obtains the following generalization of Lemma 3.16:

Lemma 3.17. *Assume that w is a braid word of length ℓ, width n, and height h. Then the number of handle reductions in any sequence of handle reductions from w is bounded above by $\ell(2h)^{2n-1}$.*

Proof (sketch). There are two key points. Firstly, when handle reduction is performed, the height of the words never increases, so it remains bounded by h. Indeed, positive and negative equivalences preserve the absolute value, while left and right reversing preserve it or, possibly, replace it by a word that is a left or a right divisor of the previous absolute value. Secondly, reducing a σ_1-handle may create new σ_2-handles, but this number is bounded by the number of σ_2 (or σ_2^{-1}) that were present in the σ_1-handle that has been reduced. As, by hypothesis, a permitted σ_1-handle includes no σ_2-handle, the number of σ_2's in a permitted σ_1-handle is bounded above by the height h, and, therefore, reducing the σ_1-handles creates at most $h+1$ new σ_2-handles.

Let us consider an arbitrary (finite, or possibly infinite) sequence of reductions starting from w. Writing N_i for the number of σ_i-reductions in this sequence, and c_i for the initial number of σ_i-handles in w, we obtain $N_1 \leqslant c_1 h$ by Lemma 3.16, then $N_2 \leqslant (c_2 + N_1(h+1))h$, and, similarly, $N_{i+1} \leqslant (c_{i+1} + N_i(h+1))h$ for every i. Using the obvious bound $c_i \leqslant \ell$, we deduce $N_i \leqslant (2^i - 1)\ell h^{2i-1}$ for each i, and the coarse bound $\sum N_i \leqslant \ell(2h)^{2n-1}$ follows. □

Inserting the previous bound on the height given by Lemma 3.14, we deduce Proposition 3.8: for every braid word w, any sequence of handle reductions from w converges in a finite number of steps with an absolute upper bound (exponentially) depending on the length and the width of w only.

Handle reduction is very easy to implement, and its practical efficiency is much better than what the proved complexity bound suggests: all experiments are compatible with a bound quadratic in the length. The following question is puzzling:

Question 3.18. *What is the true complexity of handle reduction?*

3.3. **The braid ordering.** Waht is involved in the previous results is a linear ordering on braids.

Proposition 3.19. *For x, x' in B_∞—the group defined by* (0.2) *using an unbounded sequence of generators $\sigma_1, \sigma_2, \ldots$—say that $x < x'$ holds if the braid $x^{-1}x'$ is σ-positive. Then $<$ is a linear ordering on B_∞ that is compatible with multiplication on the left.*

Proof. As the product of two σ-positive braids is clearly σ-positive, the relation $<$ is transitive. It is antireflexive as we know that 1 is not σ-positive. Hence it is a (strict) order. This order is linear, as, by Proposition 3.6, if a non-trivial braid is not σ-positive, its inverse must be σ-positive. The compatibility with multiplication follows from the definition. ☐

Corollary 3.20. *For $n \leqslant \infty$ the group B_n is an orderable group.*

Corollary 3.21. *The Artin representation of B_n is faithful.*

Proof. By Property 3.6, every non-trivial braid admits a σ-positive or a σ-negative expression. By Proposition 3.4, the automorphism associated with such a word is not the identity mapping: so the automorphism associated to a non-trivial braid is never trivial. ☐

We refer to the exercises for a few more applications.

The main further property of the braid ordering known to date is:

Proposition 3.22. [39, 14] *For each n, the restriction of $<$ to the monoid B_{n+} is a well-ordering of type $\omega^{\omega^{n-2}}$.*

3.4. **Exercises.**

Exercise 3.1. (*) Put the following braids in increasing order: σ_1, σ_2, $\sigma_1\sigma_2$, $\sigma_2\sigma_1$, $\sigma_1^{-1}\sigma_2$, $\sigma_2\sigma_1^{-1}$, $\sigma_1\sigma_2^{-1}$, $\sigma_2^{-1}\sigma_1$, $\sigma_1\sigma_2\sigma_1$.

Exercise 3.2. (*) Prove that B_n is not bi-orderable, *i.e.*, there can exist no linear ordering on B_n that is compatible with multiplication on both sides [Hint: Conjugate $\sigma_1\sigma_2^{-1}$ by $\sigma_1\sigma_2\sigma_1$.]

Exercise 3.3. (*) Give an exemple of braids x, y satisfying $x < y$ and $x^{-1} < y^{-1}$. Give an example of braids satisfying $x > 1$ and $y < xy$.

Exercise 3.4. (**) Show that the height of the braid Δ_3^{2k} is at least $2k^2$. [Hint $(\sigma_1^{2k}\sigma_2\sigma_1\sigma_2^{-2k}\sigma_1\sigma_2)^k$ is traced in the Cayley graph of $\Delta_3 2k$.] Extend to Δ_n^{2k} with height $2k^{n-1}$ at least.

Exercise 3.5. (**) Show that, for f_1, f_2 in S_n, one has $s(f_1) < s(f_2)$ if and only if the sequence $(f_1(1), \ldots, f_1(n))$ is lexicographically smaller than $(f_2(1), \ldots, f_2(n))$.

Exercise 3.6. (**) Show that the group algebra $\mathbf{C}[B_n]$ has no non-trivial zero-divisor.

Exercise 3.7. (**) Show that the group B_n is isolated in B_∞, *i.e.*, if x lies in B_∞ and x^k belongs to B_n, then x belongs to B_n.

Exercise 3.8. (**) Show that the mapping $x \mapsto x\sigma_1\partial x^{-1}$ of B_∞ into itself is injective.

Exercise 3.9. (**) Show that $(B_\infty, <)$ is order-isomorphic to $(\mathbf{Q}, <)$ (the rational numbers).

Exercise 3.10. (**) For x, y in B_∞, define the distance of x and y to be 2^{-k} where k is maximal such that $x^{-1}y$ belongs to the image of ∂^k. Show that the topology associated with $<$ is the ultrametric topology associated with the above distance.

Exercise 3.11. (**) For w a braid word, define $\mathrm{rev}(w)$ to be the word obtained by reversing the order of letters in w. Show that rev induces a well-defined anti-automorphism of B_∞. Denoting the latter by rev, show that $x \neq 1$ implies $x \cdot \mathrm{rev}(x) \neq 1$.

Exercise 3.12. (***) Assuming the (true) result that a conjugate of a braid in B_{n+} is always > 1, prove that any braid of the form $x^{-1}\partial x\sigma_1$ has a σ_1-positive expression. [Hint: Show that $x^{-1}\partial x\sigma_1$ is the product of the commutator $[x^{-1}, \sigma_2 \ldots \sigma_n]$ and of $(\partial x \cdot \sigma_1)^{-1}\sigma_1(\partial x \cdot \sigma_1)$.]

Exercise 3.13. [43] (***) Show that, for every braid x in B_n, there exists a unique integer e satisfying $\Delta_n^e \leqslant x < \Delta_n^{e+1}$. Assume x' is conjugate to x in B_n. Prove that $\Delta_n^{2e} \leqslant x < \Delta_n^{2e+2}$ implies $\Delta_n^{2e-2} \leqslant x' < \Delta_n^{2e+4}$, hence $x\Delta_n^{-4} \leqslant x' < x\Delta_n^4$.

References

[1] E. Artin, *Theorie des Zöpfe*, Abh. Math. Sem. Univ. Hamburg **4** (1925) 47–72.
[2] E. Artin, *Theory of Braids*, Ann. of Math. **48** (1947) 101–126.
[3] G. Baumslag & C.F. Miller III (eds), *Algorithms and Classification in Combinatorial Group Theory*, MSRI Publications 23, Springer Verlag (1992).
[4] D. Bessis, *The dual braid monoid*, An. Sci. Ec. Norm. Sup.; 36; 2003; 647–683.
[5] D. Bessis, *Variations on Van Kampen's method*, arXiv:math.GR/0301327.
[6] D. Bessis & R. Corran, *Garside structure for the braid group of $G(e, e, r)$*, arXiv:math.GR/0306186.
[7] M. Bestvina, *Non-positively curved aspects of Artin groups of finite type*, Geometry & Topology **3** (1999) 269–302.
[8] S. Bigelow, *Braid groups are linear*, J. Amer. Math. Soc. **14** (2001) 471–486.
[9] J. Birman, *Braids, links, and mapping class groups*, Annals of Math. Studies 82, Princeton Univ. Press (1975).
[10] J. Birman, K.H. Ko & S.J. Lee, *A new approach to the word problem in the braid groups*, Advances in Math. **139-2** (1998) 322-353.
[11] E. Brieskorn, *Automorphic sets and braids and singularities*, Braids, Contemporary Math. **78** (1988) 45–117.
[12] E. Brieskorn & K. Saito, *Artin-Gruppen und Coxeter-Gruppen*, Invent. Math. **17** (1972) 245–271.
[13] M. Broué, G. Malle & R. Rouquier, *Complex reflection groups, braid groups, Hecke algebras*, J. Reine Angew. Math. **500** (1998) 127–190.
[14] S. Burckel, *The wellordering on positive braids*, J. Pure Appl. Algebra **120-1** (1997) 1–17.
[15] G. Burde & H. Zieschang, *Knots*, de Gruyter, Berlin (1985).
[16] P. Cartier, *Développements récents sur les groupes de tresses, applications à la topologie et à l'algèbre*, Séminaire Bourbaki, exposé 716 (novembre 1989).
[17] R. Charney, *Artin groups of finite type are biautomatic*, Math. Ann. **292-4** (1992) 671–683.
[18] R. Charney, *Geodesic automation and growth functions for Artin groups of finite type*, Math. Ann. **301-2** (1995) 307–324.
[19] R. Charney, *The Tits conjecture for locally reducible Artin groups*, Int. J. of Algebra and Computation, to appear.
[20] R. Charney, J. Meier & K. Whittlesey, *Bestvina's normal form complex and the homology of Garside groups*, Geom. Dedicata; to appear.
[21] J. Crisp & L. Paris, *The solution to a conjecture of Tits on the subgroup generated by the squares of the generators of an Artin group*, Invent. Math.; 145; 2001; 19-36.
[22] J. Crisp & L. Paris, *Representations of the braid group by automorphisms of groups, invariants of links, and Garside groups*, Pac. J. Maths, to appear.
[23] P. Dehornoy, *Braids and Self-Distributivity*, Progress in Math. vol. 192, Birkhäuser.
[24] P. Dehornoy, *Complete positive group presentations*, J. of Algebra **268** (2003) 156–197.
[25] P. Dehornoy, I. Dynnikov, D. Rolfsen, B. Wiest, *Why are braids orderable?*, Panoramas & Synthèses vol. 14, Soc. Math. France (2002).
[26] P. Deligne, *Les immeubles des groupes de tresses généralisés*, Invent. Math. **17** (1972) 273–302.
[27] F. Digne, *Groupes de tresses*, Cours de DEA, http://www.mathinfo.u-picardie.fr/digne/poly_tresses.pdf
[28] I. Dynnikov & B. Wiest, *On the complexity of braids*, Preprint (2004).
[29] E. A. Elrifai & H. R. Morton, *Algorithms for positive braids*, Quart. J. Math. Oxford **45-2** (1994) 479–497.
[30] D. Epstein, J. Cannon, D. Holt, S. Levy, M. Paterson & W. Thurston, *Word Processing in Groups*, Jones & Bartlett Publ. (1992).
[31] R. Fenn, D. Rolfsen & J. Zhu, *Centralisers in the braid group and in the singular braid monoid*, Ens. Math. **42** (1996) 75–96.
[32] F. A. Garside, *The braid group and other groups*, Quart. J. Math. Oxford **20-78** (1969) 235–254.
[33] V. Gebhardt, *A new approach to the conjugacy problem in Garside groups*, Preprint, http://arxiv.org/abs/math.GT/0306199 (2003).
[34] V. Jones, *Hecke algebra representations of braid groups and link polynomials*, Ann. of Math. **126** (1987) 335–388.
[35] C. Kassel, *Quantum groups*, Springer Verlag (1995).
[36] C. Kassel, *L'ordre de Dehornoy sur les tresses*, Sminaire Bourbaki, exposé 865 (novembre 1999); Astérisque, vol. 276, Soc. Math. France, Paris 2002, 7–28.
[37] D. Krammer, *The braid group B_4 is linear*, Invent. Math. **142** (2000) 451–486.
[38] D. Krammer, *Braid groups are linear*, Ann. Math. **151-1** (2002) 131–156.
[39] R. Laver, *Braid group actions on left distributive structures and well-orderings in the braid group*, J. Pure Appl. Algebra **108-1** (1996) 81–98.
[40] D. Long, *On the linear representations of braid groups*, Trans. Amer. Math. Soc. **311** (1989) 535–561.
[41] D. Long & M. Paton, *The Burau representation is not faithful for $n \geqslant 6$*, Topology **32-2** (1993) 439–447.
[42] R. C. Lyndon & P. E. Schupp, *Combinatorial group theory*, Springer (1977).
[43] A.V. Malyutin, *Dehornoy ordering and Markov-Birman-Menasco operations*, Preprint (2002).
[44] J. Michel, *A note on words in braid monoids*, J. Algebra **215** (1999) 366–377.
[45] J. Moody, *The Burau representation of the group B_n is unfaithful for large n*, Bull. Americ. Math. Soc. **25-2** (1991) 379–384.
[46] L. Mosher, *Mapping class groups are automatic*, Ann. of Math. **142** (1995) 303–384.
[47] L. Paris, *Parabolic subgroups of Artin groups*, J. Algebra **196** (1997) 369–399.
[48] L. Paris, *Centralizers of parabolic subgroups of Artin groups of type A_ℓ, B_ℓ, and D_ℓ*, J. Algebra **196** (1997) 400–435.
[49] L. Paris, *Artin monoids inject in their groups*, Comment. Math. Helv.; 77; 2002; 609-637.
[50] M.S. Paterson & A. A. Razborov, *The Set of minimal braids is co-NP-complete*, J. of Algorithms **12** (1991) 393–408.
[51] M. Picantin, *The center of thin Gaussian groups*, J. of Algebra **245-1** (2001) 92–122.

[52] D. Rolfsen, *Braids subgroup normalisers, commensurators and induced representations*, Invent. Math. (1997) 575–587.
[53] D. Rolfsen & J. Zhu, *Braids, orderings and zero divisors*, J. Knot Th. and its Ramifications **7** (1998) 837–841.
[54] C. Rourke & B. Wiest, *Order automatic mapping class groups*, Pacific J. Math., to appear.
[55] H. Short & B. Wiest, *Orderings of mapping class groups after Thurston*, Ens. Math. **46** (2000) 279–312.
[56] W. Shpilrain, *Representing braids by automorphisms*, Intern. J. of Algebra & Comput; 11-6; 2001; 773–777.
[57] H. Sibert, *Orderings on Artin–Tits groups*, Preprint (2004).
[58] W. Thurston, *Finite state algorithms for the braid group*, Circulated notes (1988).
[59] V. V. Vershinin, *Braid groups and loop spaces*, Uspekhi Mat. Nauk **54-2** (1999) 3–84.

Laboratoire de Mathématiques Nicolas Oresme UMR 6139, Université de Caen, 14032 Caen, France
E-mail address: dehornoy@math.unicaen.fr
URL: //www.math.unicaen.fr/~dehornoy